CHAPTER 11
Protecting the Support Structure

Because of their importance to the support of tactical operations, COSCOM units and facilities remain vulnerable to attack by enemy forces. Enemy forces attempt to disrupt support activities and interdict LOCs. The COSCOM's support structure needs to be protected if corps forces are to retain their capability to surge and survive to win the corps battle.

Protection includes actions taken to offset Level I, I, and III threats. It also includes enforcing self-protective measures such as dispersal, cover, concealment, and camouflage. Units must use self-defense weaponry to fortify bases and base clusters and prevent unnecessary loss of mission supplies and equipment. Protection also includes deception actions taken to mislead the enemy as well as actions taken to secure ground LOCs and protect critical Class VII, fuel, or ammunition supply points.

THREATS TO COSCOM SUPPORT ORGANIZATIONS

Threat doctrine stresses decisive engagements to breach the main battle area and penetrate into the corps rear area to destroy high-priority targets and logistics reserves. Threat activity in the corps rear area is conducted to prepare for future threat operations or support current threat close operations. It may encompass insurgents, terrorists, sympathizers and tactical forces as well as the effects of artillery, missiles and rockets, air attacks, and radio electronic combat. FMs 102-1, 100-2-2 and 100-2-3 describe threat forces and tactics.

LEVELS OF RESPONSE

Rather than focus on the size or type of threat, units focus on the level of response required to defeat the threat. To assist commanders and staffs, PM 100-15 categorizes Level I through Level III threats by the following levels of response:

- Level I threats are those which can be defeated by base defense forces.

- Level II threats include those which are beyond the capabilities of base defense forces. These threats can be defeated by response forces, normally Ml?

- Level III threats are those which necessitate a corps command decision to commit a tactical combat force.

Since incidents do not follow a progressive sequence, commanders may face any combination of these threats at the same time. Indeed, some threat activities begin well ahead of general hostilities.

TARGETS WITHIN THE CORPS REAR AREA

An understanding of the threat to the corps rear area and detailed IPB and LPB products help to ensure protection of the support structure. Threat forces conduct operations in the corps rear area to seize and maintain the initiative, facilitate strategic and operational level penetrations, and degrade or eliminate the corps' capability to conduct coherent operations.

To achieve these aims, enemy activities in the corps rear area target –

- Chemical weapon storage sites and delivery systems.

- Corps CPs.

- Air defense artillery sites.

- Critical signal nodes.

- Critical logistics facilities and units.

- Key choke points along LOCs.

- Regeneration sites.

LEVEL I THREAT OBJECTIVES

Agents, sympathizes or terrorists attempt to create confusion, fear, or panic. They use sophisticated camera listening devices, or long-range secure radios to gain

information for exploiting vulnerabilities. They attempt to cause delay by disrupting CP operations and communications and automation networks. Individual agents or small terrorist cells conduct random attacks to sabotage logistics support operations. Enemy sympathizers conduct political demonstrations to create hostile civil strife in host countries. Reconnaissance teams conduct clandestine surveillance to gather intelligence on logistics support structure and operations. They also conduct acts against targets of opportunity.

Supporting RAOCs disseminate information to bases and base clusters on the current situation in the area, to include likely enemy targets and intentions. This information appears in the intelligence estimate and IPB products produced by the corps main CP's intelligence cell.

High priority targets include the COSCOM CP and its subordinate functional control centers. The threat attempts to disrupt CP communications nets and destroy the CSS automation management office at the COSCOM and each CSG. Petroleum and ammunition supply points as well as supply points which receive, store, or issue Class VII items present lucrative targets for sabotage. MHE may also represent a priority target. Because of the reliance of logistics units on MHE, the loss of any or all MHE impacts adversely on support provided by distribution systems.

RESPONSE TO LEVEL I THREATS

Units need to detect, isolate, minimize, and defeat Level I threats before logistics support operations become disrupted. Level I threats can be defeated by base or base cluster self-defense measures, to include OPSEC, COMSEC, and perimeter defense.

Base commanders form base defense forces. Base defense forces provide internal base security and reinforce the base perimeter when threatened.

BDOCs develop a base defense plan. They submit that plan to their designated base cluster, if applicable. BCOCs consolidate these plans and forward them to the supporting RAOC.

BDOCs/BCOCs switch organic radios to their supporting RAOC's frequency to obtain data on rear operations and the tactical situation. Units within the base/base cluster transmit Level I incidents reports both to the RAOC serving their area and to their chain of command.

LEVEL II THREAT OBJECTIVES

Level II threat objectives include command, control, and communications facilities; supply convoys; prepositioned war stocks; and reserve units marshaling in the corps rear area.

Special purpose forces, squad-size or smaller, perform reconnaissance, sabotage, and intelligence collection missions in the corps area. These forces have been trained in demolitions, communications, and languages. They often dress in HN or friendly forces uniforms or civilian clothes. They may be tasked to disrupt, destroy, or prepare for large-force incursions.

Armored reconnaissance squads airdrop into or infiltrate the corps rear area to locate reserves, monitor unit positions or movements, and conduct ground reconnaissance for avenues of approach. Other reconnaissance elements raid supply points or conduct ambushes along MSRs. Instead of attempting to seize key terrain features, assault forces focus on creating gaps to allow exploitation forces to strike deep into the corps rear area.

RESPONSE TO LEVEL II THREATS

Logistics units must use every possible measure to prevent surveillance by Level II forces. The corps rear CP's operations cell disseminates early warning information on threat airborne or air assault activities or insertions in the corps rear area. Following early warning, the operations cell notifies the RAOCs which then inform response forces and base clusters/bases.

The base cluster defense plan needs to include air, ground, and NBC attack alarm systems and describe internal air defense measures. Base defense forces prepare to detect and defeat or minimize the effects of Level I and limited Level II threat attacks against their base or base cluster.

BCOCs/BDOCs (for isolated bases) request MP assistance or supporting fires through the RAOC serving their area. The corps rear CP's operations cell designates MP elements to respond to bases or base clusters under attack by Level II threat forces.

LEVEL III THREAT OBJECTIVES

Airborne or ground infiltration forces, company to battalion-size, attempt to seize industrial complexes, key terrain, airheads, landing zones, seaports, bridgeheads, or river-crossing sites. They exploit penetrations to attack targets in the corps rear area. Level III threats attempt to disrupt command, control,

and communications facilities or to destroy preposi-tioned stocks, logistics corridors, and supply convoys.

Exploitation forces could commit before the first echelon battle ends and second echelon forces arrive. They might try to prevent withdrawal or relocation of defending units by blocking withdrawal routes and seiz-ing bridgeheads and road junctions. They might also try to destroy LOCs, seize airheads, prevent reserves moving forward, and destroy critical logistics facilities.

RESPONSE TO LEVEL III THREATS

Level III threats can be delayed or disrupted by MP response forces with supporting fires. The corps must commit a tactical combat force to defeat a Level III threat.

Logistics units report the size and intent of Level III threats to their supporting RAOC. The corps G3 task organizes a tactical combat force, normally a composite brigade-sized force, which the corps commander com-mits. All units in the TCF's area of operations become OPCON to the TCF for rear security operations.

The corps rear CP's CSS cell coordinates logistics requirements for the tactical combat force with the COSCOM support operations officer. As required, the COSCOM support operations officer directs the CMMC to divert critical supplies and services to sup-port the TCF.

SELF-PROTECTIVE MEASURES

Few COSCOM units can continue their support mis-sion while under attack, no matter how minor the threat may be. If threats continually force COSCOM units to cease mission support and take defensive actions, corps tactical operations could be effectively interrupted. To preclude continual support degradation from occur-ring, swift measures should be taken to defeat threat forces that are creating problems in the corps rear area. Passive security measures must give way to active measures in order to ensure maximum support ef-ficiency.

All soldiers must become proficient in basic tactical skills. This includes establishing perimeter defensive positions in urban areas as well as field environments. Every unit is responsible for providing its own local security. Economy of force means that all COSCOM units are responsible for defending themselves against attempts to disrupt support operations. In coordination with the MP units in their area, they employ self protec-tive measures to minimize the destructive force of enemy forces.

Self protective measures include passive measures, such as dispersion, cover, concealment and camouflage. Often, merely avoiding detection serves as the best defense. Self protective measures also include active measures, such as —

- Using crew-served weapons and preparing in-dividual positions.

- Emplacing obstacles.

- Placing SAWS in key positions to protect base cluster perimeters and critical stockage points.

- Adjusting indirect fires.

- Reacting to air, NBC, and indirect fire attacks.

DISPERSION

Organizing units into a defensive 360-degree perimeter absorbs manpower and provides only a thin line of protection. Once penetrated, the perimeter remains nearly impossible to re-form.

Point defense of functional small unit areas, with the fullest possible use of unit dispersion, has evolved as the most practical method of defense. Instead of manning the entire perimeter, logistics units form reaction forces to defend critical elements. The enemy could even pass through the base cluster area without hitting any defended point.

To reduce the vulnerability of the corps' GS support-ing base, logistics organizations traditionally disperse similar type units throughout the corps rear area. Dis-persion helps to avoid catastrophic damage from air, artillery, and mass destruction weapons. Even if a logis-tics unit was not listed as a primary target, it could become an excellent target of opportunity. The disper-sion required depends on the —

- Type of Threat. The probability of attack by air, as an example, requires greater dispersion than an attack by small units.

- Terrain. Occupying urban terrain decreases dis-persion requirements because of the cover provided by buildings in built-up areas. Road networks with increased access which can bear expected traffic loads allow for greater dispersion of elements.

- Access to Supported Customers. Increased dispersion of COSCOM units decreases the ease of access by customers. However, dispersing classes of supply throughout the corps rear area provides customers with one-stop support at several locations.

- Defensibility. Dispersion also depends on the ability of a unit to prevent, resist, or defeat enemy forces. Normally, units defend themselves better in built-up areas. In the field, defensibility improves as dispersed units withdraw to form closely knit base clusters.

COVER, CONCEALMENT, AND CAMOUFLAGE

Logistics resources that cannot be detected cannot be targeted. Cover, concealment, and camouflage remain critical to protecting logistics units, facilities, and supplies from enemy detection and attack.

- Cover includes natural and artificial protection from enemy observation and fire. When selecting sites, advance parties need to consider the type of cover available for fighting positions and logistics resources. When available, engineers provide hardened sites for critical logistics resources.

- Concealment includes natural or artificial protection from enemy detection. COSCOM units need to conceal customer access areas as well as unit signature and mission equipment. Smoke may be used to conceal activities and to deceive the threat.

- Camouflage consists of using natural or artificial materiel, objects, or tactical positions to confuse, mislead, or evade the enemy. With the exception of medical units, logistics units use camouflage to conceal operations and the identity of critical assets. (According to FM 8-10 and STANAG 2931, camouflage of a medical unit, vehicle, or aircraft on the ground results in the loss of the protective status afforded by the Geneva convention.) Use of extensive camouflage nets may prevent the enemy from determining the type of logistics support element. TM 5-200 describes field techniques for preparing camouflage materials. FM 5-20 covers engineer camouflage operations.

INTELLIGENCE GATHERING

Logistics units use observation posts, listening posts, or unattended ground sensors on likely avenues of approach to collect intelligence on threat activity. In areas where the populace remains friendly, local law enforcement or government agencies can provide information

on threat activities in the area. BCOCs implement an integrated warning plan within their cluster and with adjacent bases or base clusters. G2/S2 personnel transmit intelligence data and IPB products over rear operations nets.

DIRECT/INDIRECT FIRE PLAN

It is always difficult to identify enemy troops at any distance. Logistics units need to preplan targets for artillery support. However, artillery support may not be timely. Clearances to fire artillery in the corps rear area must be closely controlled to prevent firing on friendly forces.

RAOCs assist group and battalion rear operations branch personnel develop direct/indirect fire plans. These fire plans need to identify –

- Probable enemy avenues of approach.

- Probable engagement areas.

- Target reference points.

- Priority of defense for support elements.

- Fire support request and coordination measures with designated fire support element.

OBSTACLES

Obstacles slow, impede, or channel enemy movement and incursions. They buy time until reaction forces can deploy or a response force can arrive. Effective use of obstacles involves sound countermobility planning and early warning.

Countermobility Plan

S2/3 staff officers in COSCOM organizations develop countermobility plans. These countermobility plans need to identify –

- Obstacle constraints and restrictions using the COSCOM OPLAN.

- Possible obstacle locations and type of obstacles.

- Available obstacle assets, to include real and artificial mine devices.

COSCOM Staff Support

The COSCOM ACofS, G3's rear operations/ADC branch coordinates obstacle support requirements with the supporting corps engineer element.

REACTION FORCE

Subordinate battalion commanders designated as base/base cluster commanders organize and train a reaction

force to provide base/base cluster defense of selected support elements. When enemy forces exceed base and base cluster defense capabilities, response forces provide the initial force to close with and destroy the enemy. The reaction force should be armed to deliver the greatest possible volume of fire using unit resources. It commits on the order of the base/base cluster commander. S4 staff officers coordinate reaction force equipment and supply requirements.

AIR DEFENSE

Air attack is perhaps the greatest single threat to logistics units in the corps rear area. Threat air forces may include attack helicopters, attack aircraft, and fighter bombers. Attack helicopters employ in support of threat offensive airborne or heliborne operations in the corps rear area. When necessary, helicopters attack missiles being transported or in firing positions. They attack C2 facilities and air assets on the ground. They also conduct raids and ambushes.

The best air defense measure consists of avoiding being detected from the air. This is accomplished by innovative use of natural terrain or by using camouflage nets.

Each soldier receives training in small arms air defense techniques, to include visual identification of hostile aircraft. If soldiers fire in mass, small arms can bring slow, low flying aircraft down.

COSCOM Staff Support

The COSCOM OPLAN establishes air defense policies. It includes corps directives on firing at aircraft. COSCOM ACofS, G3 staff officers plan for engineer hardening of critical positions. They coordinate with the corps air defense elements in determining air defense priorities for critical support elements. Depending on the intensity of the air threat, priority of corps critical assets, and availability of air defense assets, the corps G3 task organizes ADA assets under the corps rear CP. The rear CP's operations cell coordinates ADA coverage with the supporting ADA unit to provide as much coverage of the prioritized list of critical assets as possible.

Early Warnings

The corps rear CP's operations cell disseminates air defense early warnings through the rear command net. Most COSCOM units receive air defense warnings through the tactical chain of command.

NBC DEFENSE

Commanders continually examine and adjust the degree of risk that they can accept with respect to their support mission. Chapters 4 through 8 of this manual describe the possible impact of NBC attacks on logistics missions. Each unit FSOP includes information on planning and conducting NBC defense. All unit personnel receive training in —

- Contamination avoidance measures, to include NBC reconnaissance, detection and warning of NBC hazards, and measures to limit the spread of contamination.

- Protective measures, to include wearing MOPP gear, recognizing NBC alarms, and administering self aid and buddy aid.

- Decontamination operations, such as emergency or partial decontamination of personnel and equipment. (Chemical decontamination units perform deliberate decontamination of equipment.)

BATTLEFIELD DECEPTION

Logistics units use battlefield deception measures to conceal or falsify unit disposition and support capabilities.

STAFF RESPONSIBILITIES

The corps G3's battlefield deception cell plans the deception story and prepares the deception annex to the corps OPORD. Based on the corps deception plan, the corps rear CP tasks the COSCOM to execute deception events and employ deception devices and decoys. COSCOM ACofS, G2 intelligence staff officers prepare the deception annex to COSCOM OPLANs and OPORDs. FMs 34-60 and 90-2 detail staff responsibilities in support of battlefield deception plans.

ELECTRONIC DECEPTION

Electronic deception techniques help deceive EW reconnaissance elements and force the enemy to use up some of their intelligence, jamming, and deception assets. Techniques which COSCOM units may use to mislead enemy forces relative to the size, activity, and location of supporting as well as supported units include —

- Transmitting preplanned messages containing false information on support capabilities.

- Using dummy codes in valid LOGSTAT messages.

- Routing messages to other stations in the COSCOM command/administrative logistics net to create the impression that all units in the net appear equally committed.

- Maintaining periods of radio silence to create the impression of forthcoming unit movements.

- Creating the impression of unusual logistics support activity.

- Transmitting unit signatures from false locations, while suppressing signatures from actual locations.

LOGISTICS DECEPTION

Deception techniques help conceal logistics facilities or hide vehicular movements associated with receipt, storage, and issue operations. In support of the corps deception plan, COSCOM ACofS, G3 staff officers could task subordinate units to use one or more of the following deception techniques:

- Use houses and factory buildings to conceal supply, field services, maintenance, and transportation support operations.

- Disguise containers and packages to resemble those used by civilian suppliers.

- Set up supply points in unorthodox positions.

- Use empty fuel drums and ammunition boxes to help represent supply point activity where none exists.

- Use training exercise recordings of logistics unit activity to simulate the presence or movement of logistics support activities.

- Establish deception supply routes.

- Use civilian trucks, buses, and cars to transport supplies.

- Simulate the evacuation, abandonment, or destruction of supplies and equipment.

- Use unserviceable items, salvage, or combat loss items as decoys.

REAR SECURITY

The rear CP's operations cell and subordinate RAOCs plan and conduct rear security operations. RAOCs designate base/base cluster commanders and form bases and base clusters to increase security. The rear CP's CSS cell identifies key logistics units or supporting activities which require priority protection. For example –

- Critical Class V and III resupply convoys require special protection by MP or maneuver forces.

- Air defense assets need to accompany critical convoys or be prepositioned along the supply route.

- Aerial resupply missions require army aviation support.

BASE/BASE CLUSTERS

RAOCs group units into either bases or base clusters to increase mutual security, take advantage of limited communications assets, and conduct a sustained defense against attacks. This decreases the rear operations commander's span of control.

RAOCs ensure that bases and base clusters develop viable self-defense plans. Their primary concerns are the positioning of units within their area of responsibility and the control of Level I responses to enemy activity.

RAOCs also provide continual threat information to units within their AO.

The COSCOM headquarters, CMMC, CMCC, and the corps rear CP are normally grouped into a base. In addition, if the tactical combat force is a dedicated force, its CP collocates with the corps rear CP to facilitate coordination. An MP combat support company prioritizes and integrates the corps rear CP, TCF CP COSCOM HHC, and centers into its area security plans. It occupies key terrain around the COSCOM and corps rear CP site and conducts screening type operations to prevent infiltration into the area.

AR 600-20 prohibits a medical unit commander from commanding a base or base cluster containing nonmedical units. MP commanders are avoided due to their response force mission. FM100-15-1 directs that RAOCs avoid designating group and higher headquarters as base or base cluster commanders. However, the RAOC may designate COSCOM battalion commanders as the base/base cluster commander.

Base commanders are responsible for –

- Ensuring all personnel receive training in the basic defense techniques needed to establish a viable defense.

- Preparing a base defense plan.

- Rehearsing all personnel and units within the base on the effective execution of the base defense plan.

- Organizing a reaction force.

- Recommending movement or repositioning of the base to enhance security.

- Coordinating mutual support from bases in or near their vicinity.

- Coordinating response force operations.

- Adjusting base defenses as the threat changes.

- Determining the defense status of the base.

COSCOM ACofS, G3 and CSG S3 staff officers ensure that battalion personnel are well trained in base or base cluster defense operations.

Base Defense Operations Center

The base commander establishes a BDOC to plan, coordinate, and supervise base defense operations. He draws personnel and equipment from tenant units to form a functional BDOC. BDOC tasks include –

- Ensuring the base perimeter is defined and that responsibilities for sectors are established.

- Ensuring wire communications are established.

- Increasing/decreasing the defensive posture based on threat operations.

- Developing and monitoring the base defense plan.

- Monitoring and reporting base defense status.

Base Cluster Operations Center

The base cluster commander establishes a BCOC. The BCOC interfaces with the sector RAOC. BCOC tasks include –

- Developing the base cluster defense plan.

- Coordinating with the RAOC for fire support, reaction forces, and response force assistance.

- Maintaining continuous communications with the area RAOC and assigned bases.

- Receiving and passing base defense status reports.

- Receiving and passing information on the threat.

Each base or base cluster maintains organic radio equipment dedicated to the rear operations net. The BCOC uses that net to maintain communications with subordinate bases, adjacent clusters, and the supporting RAOC.

Base/Base Cluster Defense Plan

Each base/base cluster commander develops and implements a comprehensive defense plan to defend their sites and protect their support capabihy. The defense plan includes measures to detect, minimuze, or defeat Level I and limited Level II threat attacks. To maximize mutual support and prevent fratricide, the sector RAOC coordinates the defense plans with adjacent bases/base clusters and joint, combined, and HN forces. The rear CP's operations cell integrates these defense plans into an overall corps rear fire support plan.

RESPONSE FORCES

The corps rear CP's operations cell designates corps response forces to respond to base/base clusters under attack by Level II threat forces. The corps relies on the MP brigade for response forces. It augments the brigade with combat and CS assets as available. Fire support assets in support of MP response forces consist of artillery or Army aviation. They are placed OPCON to the MP brigade when dedicated.

The corps designates other backup or alternative response forces when MP elements are unavailable for commitment in sufficient strength for response force operations. Response force options include engineer units, chemical units, transiting combat units, and elements of the reserve or HN assets if available. The corps rear CP coordinates with the corps G3 prior to committing other than MPs to response force missions. These optional forces are placed OPCON to the MP brigade to ensure unity of effort.

Response forces position themselves to best interdict enemy forces en route to key corps facilities or to best respond to an attack on priority facilities. The operations cell coordinates with the corps FSCOORD for fire support of response forces. If unable to defeat an enemy force, response forces maintain contact with the enemy force to delay or disrupt the enemy until the corps commits a TCF.

TACTICAL COMBAT FORCE OPERATIONS

The primary mission of a TCF is to defeat threat forces in the corps rear area that exceed the capability of the MP brigade. The G3 designates a TCF capable of defeating Level III forces in the corps rear area and within divisional rear areas. The size and composition of the TCF varies based on the corps rear area IPB and

METT-T analyses. The TCF supports an on-order or dedicated rear operations mission.

The corps commander does not normally commit the TCF until the rear operations commander determines that base cluster defense forces and or response forces cannot counter the threat. Once committed, all units within the TCF's designated area of operations become OPCON to the TCF for rear security operations until forces defeat the threat.

FIRE SUPPORT

Response forces and the TCF require timely fire support to ensure the defeat of the rear threat. The corps rear CP plans rear area fire support. The fire support element at the corps rear CP continually monitors available fire support assets. Units passing through or being reconstituted in the corps rear area which posses artillery or mortar could provide limited fire support to assist critical bases/base clusters counter threat incursions. The fire support must fit the approved tire plan and restrictive fire coordination measures.

Armed or attack helicopters provide fire support for based/base clusters, response forces, and TCF. The corps rear CP establishes request and fire direction channels for Army aviation assets.

AIR DEFENSE

Depending on the intensity of the air threat and availability of air defense assets, the corps rear CP's operations cell coordinates air defense coverage along MSRs to protect critical nontactical convoys from air attack. Adjacent or transiting units may provide fire support to combat Level II and III threats.